IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Norfolk Division

IN THE MATTER OF THE SEARCH OF:	)	**FILED UNDER SEAL**
	)	
1216 IVYSTONE WAY APT 305 CHESAPEAKE, VA 23320;	)	Case No. 2:22-sw-81
	)	
The person of AARON GONZALES;	)	Case No. 2:22-sw-82
	)	
2008 green TOYOTA PRIUS, Bearing VA license plate OD4080; and	)	Case No. 2:22-sw-83
	)	
The Google account of aaronpaulgonzales12@gmail.com	)	Case No. 2:22-sw-84

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

Introduction and Agent Background

I, John W. Shields, being duly sworn, hereby depose and state:

1. I am a Special Agent (SA) with the United States Department of Homeland Security - Homeland Security Investigations ("HSI") assigned to Norfolk, Virginia. I have been an Agent with HSI since April 2016. I am currently assigned to the Child Exploitation and Human Trafficking Group, which conducts a wide variety of investigations of crimes including crimes where computers and the internet are used in the sexual exploitation of children, including (but not limited to) violations involving producing or trafficking in child sexual abuse material ("CSAM"). In addition to working on Federal investigations, I have worked on child molestation/child sex abuse cases while working for the Lincoln County Sheriff's Office and the Reardan Police Department in Washington State. In connection with my work in both local and federal law enforcement, I have received formal and on-the-job training in the investigation of cases involving the sexual exploitation of children to include training programs, participation in the execution of

search warrants involving CSAM, and participation in warrants involving seizures of computers and other digital storage media. In addition, I have conducted numerous drug smuggling investigations resulting in the seizure of contraband and the arrest of numerous suspects. The statements contained in this Affidavit are based on my experience and background as a Special Agent and on information provided by other law enforcement agents.

2. As such, I am an "investigative or law enforcement officer of the United States" within the meaning of 18 U.S.C. § 2510(7). That is, I am an officer of the United States, empowered by law to conduct investigations regarding violations of United States law, to execute warrants issued under the authority of the United States, and to make arrests of the offenses enumerated in, among others, 18 U.S.C. §§ 2252 and 2252A. In the course of my duties, I am responsible for investigating crimes which include, but are not limited to, child exploitation and CSAM.

3. The information set forth in this affidavit is known to me as a result of an investigation personally conducted by me and other law enforcement agents. Thus, the statements in this affidavit are based in part on information provided by Special Agents and other employees of HSI, as well as other investigators employed by federal or state governments. I have participated in investigations involving persons who collect and distribute CSAM, and the importation and distribution of materials relating to the sexual exploitation of children. I have received training in child exploitation, and I have reviewed images and videos of CSAM in a wide variety of media forms, including computer media. I have also discussed and reviewed these materials with other law enforcement officers.

4. In the course of my employment as a sworn law enforcement officer, I have participated in the execution of numerous search warrants resulting in the seizure of computers,

magnetic storage media for computers, other electronic media, and other items evidencing violations of state and federal laws.

5. This affidavit is made in support of an application for a warrant to search the entire premises located at are **1216 Ivystone Way Apartment 305, Chesapeake, Virginia** (the SUBJECT PREMISES). Additionally referenced in this affidavit **Aaron Gonzales** (GONZALES), a **2008 green Toyota Prius bearing VA License Plate OD4080** (the SUBJECT PRIUS), and a Google account, aaronpaulgonzales12@gmail.com (GOOGLE ACCOUNT). The SUBJECT PREMISES, GONZALES, the SUBJECT PRIUS, and the GOOGLE ACCOUNT are more precisely described in Attachments A-1 through A-4, for items specified in Attachments B-1 through B-4. Regarding the GOOGLE ACCOUNT, Google is a provider of electronic communications services based in Mountain View, California, respectively.

6. This affidavit is based upon information that I have gained from my investigation, my training and experience, as well as information gained from conversations with other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities (more precisely described in Attachments B-1 through B-4) of violations 18 U.S.C. §§ 2252(a)(2) and (4)(B) are located in, at, or on the SUBJECT PREMISES, GONZALES, SUBJECT PRIUS, and the GOOGLE ACCOUNT.

Pertinent Federal Criminal Statutes

7. This investigation concerns alleged violations of 18 U.S.C. §§ 2252(a)(2) and (4)(B), relating to material involving the sexual exploitation of minors.

8. 18 U.S.C. § 2252(a)(2) prohibits a person from knowingly receiving or distributing, using any means or facility of interstate or foreign commerce or that has been mailed, shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed, shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails, any visual depiction of minors engaging in sexually explicit conduct.

9. 18 U.S.C. § 2252(a)(4)(B) prohibits a person from knowingly possessing, or knowingly accessing with intent to view, one or more books, magazines, periodicals, films, or other materials which contain visual depictions of minors engaged in sexually explicit conduct that have been mailed, shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed, shipped or transported, by any means including by computer.

Definitions

10. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

11. "Child pornography," as defined in 18 U.S.C. § 2256(8), or "Child Sexual Abuse Material," is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual

depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

12. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device," and includes smartphones, and mobile phones and devices. See 18 U.S.C. § 1030(e)(1).

13. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

14. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alphanumeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or

"booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

15. "Contents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication. 18 U.S.C. § 2510(8).

16. "Electronic Communication Service" refers to any service, which provides to users thereof the ability to send or receive wire or electronic communications. 18 U.S.C. § 2510(15).

17. "Electronic Communications System" means any wire, radio, electromagnetic, photo optical, or photo electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications. 18 U.S.C. § 2510(14).

18. "Electronic storage" means (a) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (b) any storage of such communication by an electronic communication service for purposes of backup protection of such communication. 18 U.S.C. § 2510(17).

19. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

20. "Internet Protocol Address" (IP Address), as used herein, refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the

Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

21. "Minor" and "sexually explicit conduct" are defined in 18 U.S.C. §§ 2256(1) and (2). A "minor" is defined as "any person under the age of eighteen years." The term "sexually explicit conduct" means actual or simulated:

a. Sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;

b. Bestiality;

c. Masturbation;

d. Sadistic or masochistic abuse; or

e. Lascivious exhibition of the genitals or pubic area of any person.

22. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

23. "Remote Computing Service" is a service that provides to the public computer storage or processing services by means of an "electronic communications system." 18 U.S.C. § 2711.

24. "Secure Hash Algorithm" (SHA-1) is one of a number of cryptographic hash functions published by the National Institute of Standards and Technology as a U.S. Federal Information Processing Standard. SHA-1 is the original 160-bit hash function. It was designed by the National Security Agency (NSA) to be part of the Digital Signature Algorithm. The SHA-1 value is one form of an electronic fingerprint for a digital image.

25. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

Use of Computers with Child Sexual Abuse Material

26. Based upon the information officially supplied to me by other law enforcement officers, I know the following:

a. Computers and digital technology have dramatically changed the way in which individuals interested in CSAM interact with each other. Computers basically serve four functions in connection with CSAM: production, communication, distribution, and storage.

b. Those interested in CSAM can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, including those included in a smartphone or mobile phone, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded

video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to millions of computers around the world via the Internet. The ability to produce CSAM easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. CSAM can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for CSAM. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or

"flash" drives, which are very small devices, which are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading CSAM in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store CSAM, including services offered by Internet Portals such as Yahoo! and Gmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of CSAM can be found on the user's computer or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained

unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

Probable Cause

27. On 07/26/21, HSI Cyber Crimes Center received an intelligence report from the UK National Crime Agency. The UK National Crime Agency was reporting two Kik users who from 06/02/21 to 07/14/21 were chatting with a subject the users appeared to believe to be a 12-year-old girl. The first reported Kik user was "Funtimes1163," who Kik reported listed their contact email as the GOOGLE ACCOUNT, aaronpaulgonzales12@gmail.com.[1] "Funtimes1163" had a Display Name of 'The Wonderful'. "Funtimes1163" frequently accessed Kik through IP address 68.131.82.156 between 06/14/2021 and 07/14/2021. "Funtimes1163" purported to be a 27-year-old male from Florida. "Funtimes1163" communicated with the purported minor about sexual topics, including asking if the minor masturbated. "Funtimes1163" also claimed to date other minors. "Funtimes1163" talked about how he works in "Jewelry."

28. The second reported Kik user was "notmenoryou69". "notmenotyou69" frequently accessed the Kik network though the same IP address as "Funtimes1163" between 06/18/2021 and 07/14/2021. Kik reported the account with username "notmenotyou69" listed their contact email as funtimes1163@yahoo.com. "notmenoryou69" claimed to be a 15-year-old girl named Nancy

[1] As a matter of practice, Kik sends emails about their account and requests to verify users' information to the user's reported email address.

who lived in Florida. "notmenoryou69" also claimed to be dating "Funtimes1163". "notmenoryou69" also engaged in conversation of a sexual nature with the purported 12-year-old.

29. Based on analysis of the IP addresses used by both "Funtimes1163" and "notmenoryou69," as well as the fact that the email listed by "notmenoryou69" is funtimes1163@yahoo.com, which is derived from the username of the first reported account, I believe both of the users are in fact one person.

30. On 01/03/22 the National Center For Missing and Exploited Children (NCMEC) received a report from MediaLab AI Inc., the parent company for the Kik messaging application. MediaLab reported a Kik user who uploaded 78 files of apparent child pornography and child erotica, and stated that the Electronic Service Provider viewed the entire contents of the uploaded files. The user screen name reported was notmenotyou69 with an email address of funtimes1163@yahoo.com. This user was reported to have uploaded the 78 files between 12/01/21 and 12/18/21. The uploads occurred in both group chats and private chats. NCMEC generated Cybertipline Report 114383039 and forwarded the information to HSI.

31. A review of the information provided showed 45 of the files were uploaded on multiple dates between 12/01/21 and 12/18/21 from the same IP address, 68.131.82.156 (which is also the same IP address used by both users in the earlier activity reported by the UK National Crime Agency, which is registered to Verizon. An HSI Special Agent issued a summons to Verizon to identify the account that this IP address was assigned. Verizon responded identifying that account that was assigned 68.131.82.156 belonged to Aaron GONZALES with a service address of the [redacted], Chesapeake, Va 23322. The IP address was initially assigned to the account on 12/13/2019 and was still the active IP address on the account as of January 28th, 2022.

32. I reviewed the files Kik had submitted to NCMEC. I observed the 78 files appeared to be child pornography or child erotica images and videos. Three examples of the files are more particularly described below:

a. 823db6a7-4444-4b89-b295-6732af04c482.mp4 is a one minute 22 second video that depicts a side view of a 5 to 7 year-old girl performing oral sex on what appears to be an adult male penis.

b. 6c699a88-d8b7-490f-add9-d06d47fa9c50.mp4 is a 59 second video that shows a three to four year old girl naked in a bath tub with a naked adult male. The child uses both hands to stoke a naked adult male penis.

c. 60d8c6d7-87f4-4f41-b846-f65c5985f606.mp4 is a one minute 22 second video that shows a girl who is about five years old naked with "fuck me" and an arrow pointing to the vagina of the child written on her stomach and pelvic area, being vaginally penetrated by an adult male.

33. Law enforcement databases as of May 6th 2022, showed two known adult residents of [redacted] Aaron GONZALES and a female adult, M.G./S. (hereinafter, "M.G."). Databases show GONZALES has a date of birth of [redacted]/1985 and is currently employed by Finks Jewelry. M.G. has a appears to be working at Sentara Norfolk General Hospital as a Licensed Practical Nurse. A review of M.G.'s publicly available social media revealed a family photo with both she and GONZALES along with what appeared to be three minor children.

34. I spoke to a detective of the Chesapeake Police Department (CPD), who confirmed there have been no CPD involvements with the [redacted]. since 2016; involvements prior to 2016 did not list the GONZALES family as involved parties. The detective also advised that their records show three juveniles living at the residence: [redacted]

[redacted].

35. I began periodic surveillance of [redacted]. On May 6,2022, at about 5:45 PM, I observed two vehicles in the driveway of the residence. One of the vehicles was a 2016 Acura SUV bearing Virginia license plate VSC1724. The Acura registered owners are listed as M.G. and GONZALES at [redacted]. The second vehicle was a 2015 Ford bearing Virginia license plate TZL8991. The Ford is registered to M.G. at [redacted].

36. On May 13, 2022, at about 06:28 AM, I observed the SUBJECT PRIUS parked in the driveway of [redacted]. The SUBJECT PRIUS is registered to M.G. at [redacted].

37. On May 19, 2022, I and a HSI Task Force Officer were conducting surveillance at the [redacted] All three known vehicles were observed. At about 07:45 AM, M.G. exited the house with a minor child and both got into the Acura SUV. Additionally, GONZALES exited the house just after the previous two and got into the SUBJECT PRIUS. Both vehicles left [redacted]. at about 07:50 AM. We followed GONZALES to a nearby Kroger Grocery store. GONZALES put gas in the Prius and then entered the grocery store where he purchased a drink. GONZALES then drove to Finks Jewelry Store. GONZALES sat in the SUBJECT PRIUS for several minutes in the parking lot in front of the store. GONZALES was observed and photographed while he appeared to be watching content on a cellphone or small tablet. GONZALES exited the SUBJECT PRIUS and entered Finks Jewelry at about 08:58 AM. On multiple occasions I saw Gonzales use a phone while driving and while sitting in his car in a parking lot. JWS LRL

38. On June 8, 2022, a HSI Task Force Officer and I conducted surveillance at [redacted] I observed the white Ford registered to M. G. in the driveway. At about 8:06 AM the Task Force Officer observed a middle-school-aged female exit [redacted] and walk to a school bus stop in front of [redacted] At about 8:16 am the Task Force Officer observed a high-

school-aged male exit [redacted] and walk to a school bus stop in front of the residence. We did not see the SUBJECT PRIUS at the residence or at Finks Jewelry store. We continued periodic surveillance of [redacted] over the next several days but did not see the SUBJECT PRIUS return.

39. On June 15, 2022, a law enforcement database indicated the SUBJECT PRIUS was parked on Ivystone Way, near the SUBJECT PREMISES. I conducted surveillance at The Amber at Greenbrier Apartments, which is the apartment complex where the SUBJECT PREMISES are located. I observed GONZALES enter the leasing office/clubhouse with his minor son, H.K.. About ten minutes later, they left the leasing office and walked to building 1216 and went up at least two flights of stairs, towards the SUBJECT PREMISES.

40. On June 16, 2022, I issued a summons to Bonaventure Property Management on the manager of The Amber at Greenbrier Apartments. Bonaventure responded indicating GONZALES signed a lease for apartment 1216-305 at the SUBJECT PREMISES on June 13, 2022. GONZALES listed his email as the GOOGLE ACCOUNT on his application. Additionally, GONZALES listed his marital status as separated.

41. On or about June 21, 2022, Yahoo! responded to an 18 U.S.C. § 2703(d) order for the account associated with funtimes1163@yahoo.com that the email is not an active account and that they could not provide subscriber information.

Characteristics of Collectors of Child Sexual Abuse Material

42. Through my discussions with law enforcement officers who specialize in the investigation of child pornography, and of subjects who use the Internet and Peer-to-Peer file sharing software technologies ("P2P") to gain access to CSAM, along with my training and experience, I have learned and know that individuals who use such technology are often collectors.

Moreover, I have learned that many subjects have saved numerous images and videos to their hard drive, thumb drive, disks or CDs, and have kept that material for long periods of time. Based upon my knowledge, experience and training in CSAM investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of CSAM:

a. CSAM collectors may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, in other visual media or from literature describing such activity.

b. Collectors of CSAM may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, drawings, or other visual media. CSAM collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to "groom" or lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Collectors of CSAM typically possess and maintain their "hard copies" of material, that is, their pictures, films, videotapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. CSAM collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica,[2] and videotapes for many years.

---

[2] According to former FBI Special Agent Kenneth V. Lanning, the author of a chapter in the book, Child Pornography and Sex Rings, (Lexington Books 1984), a book which deals with the subject of child pornography and pedophiles who collect and produce child pornography, "child

d. Likewise, CSAM collectors often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.

e. CSAM collectors also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests.

f. CSAM collectors typically prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in CSAM investigations throughout the world.

43. I believe that a user of the mentioned IP Addresses, at the SUBJECT PREMISES, possesses characteristics common to individuals who access with the intent to view and possess, collect, receive, distribute child pornography. I reach this conclusion because:

44. The files of interest described in the preceding paragraphs were shared over several weeks, allowing those files to be available for download by any other P2P user on the particular

---

erotica" are materials or items which are sexually arousing to pedophiles but which are not in and of themselves obscene or which do not necessarily depict minors in sexually explicit poses or positions. He defines it in the above book as: any material, relating to children, that is sexually arousing to a given individual...[s]ome of the more common types of child erotica include photographs that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids. Id. at 83.

network, and the user of the mentioned IP Address shared numerous files of interest that contained child pornography.

45. Given the behavior commonly observed among CSAM collectors, and based on my training, experience, and the facts described in the preceding paragraph, there is probable cause to believe the target of this investigation continues to possess CSAM.

BIOMETRIC ACCESS TO DEVICES

46. This warrant permits law enforcement to compel GONZALES to unlock any electronic devices requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress GONZALES' thumb and/or fingers on the device(s); and (2) hold the device(s) in front of GONZALES' face with his eyes open to activate the facial-, iris-, and/or retina-recognition feature.

Conclusion

47. Based on the facts set forth above, I believe probable cause exists that GONZALES, who resides at the SUBJECT PREMISES, has violated 18 U.S.C. §§ 2252(a)(2) and (4), which prohibit the knowing receipt or distribution of child pornography in interstate or foreign commerce, and the knowing possession of material containing an image of child pornography that has traveled in interstate or foreign commerce or was produced using material so transported or shipped.

48. I further submit that probable cause exists to believe that evidence, fruits, and instrumentalities (more precisely described in Attachments B-1 through B-5) of such violations will be found at the SUBJECT PREMISES, on GONZALES, in the SUBJECT PRIUS, and in the GOOGLE ACCOUNT (more precisely described in Attachments A-1 through A-4).

49. Accordingly, I request that a search warrant be issued authorizing HSI agents, representatives of HSI, with assistance from representatives of other law enforcement agencies as required, to search the place, person, vehicle, and accounts specified in Attachments A-1 through A-4, for the items specified in Attachments B-1 through B-4. As to the GOOGLE ACCOUNT, because the warrant will be served on Google electronically or by mail, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

FURTHER AFFIANT SAYETH NOT.

John W. Shields
Special Agent
Department of Homeland Security
U.S. Immigration and Customs Enforcement
Homeland Security Investigations

Subscribed and sworn before me this 23rd day of June, 2022 in the City of Norfolk, Virginia.

Honorable Lawrence R. Leonard
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-1

SUBJECT PREMISES

DESCRIPTION OF THE PREMISES TO BE SEARCHED

Property to be Searched: 1216 IVYSTONE WAY APT 305, CHESAPEAKE, VA 23320

The Subject Premises to be searched is the property described **1216 IVYSTONE WAY APT 305, CHESAPEAKE, VA 23320** and includes any outbuilding, storage space, basement, treehouse, garage, or vehicles located on the property.

The residence is further described as a third story apartment with a white door in building 1216 on Ivystone Way. The numbers on the door "305" are located in white on a black plaque located in the middle of the door.

ATTACHMENT B-1

DESCRIPTION OF ITEMS TO BE SEIZED

The items to be seized are evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B), and include the following:

1. Records, documents, materials, videos, and photographs, pertaining in any way to child pornography and visual depictions of minors engaged in sexually explicit conduct (hereinafter collectively referred to as "child pornography"), child erotica, and materials pertaining to an interest in child pornography, in whatever format found.

2. Records, documents, materials, and correspondence pertaining to the possession, receipt or distribution of child pornography, and any records indicating whether such was transmitted or received using a computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail.

3. Records, documents, materials, envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, seeking to obtain and/or offering to transmit child pornography through interstate or foreign commerce, including U.S. mail or by computer.

4. Records, documents, materials, envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, identifying persons transmitting or offering to transmit any visual depictions of minors engaged in sexually explicit conduct and any records identifying the means of such transmission.

5. Records, documents, materials, and photographs depicting sexual conduct, whether between adults and minors or between minors.

6. Records, documents, materials evidencing occupancy or ownership of the premises to be searched, including but not limited to, utility bills, mail envelopes, or addressed correspondence.

7. Records, documents, materials or other items which evidence ownership or use of computer and electronic equipment found in the above residence, including but not limited to, sales receipts, bills for Internet access, records containing account/user names and passwords, handwritten notes, and handwritten notes in computer manuals.

8. Records, documents, and materials pertaining to the production, reproduction, receipt, shipment, ordering, soliciting, trading, purchasing, or transactions of any kind involving the transmission through interstate or foreign commerce, including by U.S. mail or other common carrier or by computer or electronic device, of child pornography.

9. Records, documents, and materials, including but not limited to bank, financial, and credit card records, pertaining to the purchase of materials or access to materials containing child pornography.

10. Computer hardware, including central processing units (CPUs), computer software and programs, laptop computers, monitors, keyboards, printers, computer disks (including floppy disks, CDs, DVDs), scanners, disk drives, modems, routers, magnetic storage media, thumb or flash drives, memory sticks, PDAs, digital cameras and memory cards, cell phones, smartphones, I-Phones, I-Pods, I-Pads, electronic notebooks and tablets, hardware and software operating manuals, post-it notes, records containing account/user names and passwords, and other computer-related and/or electronic equipment and/or digital media, to be inspected off-site using appropriate mirror-imaging and other equipment after seizure, which are used as instrumentalities of the crimes noted or which contain any of the items noted in paragraphs 1-9 above.

11. Any of the items described in paragraphs 1-10 above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer or with the aid of computer-related equipment, including floppy diskettes, fixed hard drives, removable hard drives, software, PDAs, cell phones, or memory in any form, to be inspected off-site using appropriate mirror-imaging and other equipment after seizure.

During the execution of this search warrant, law enforcement is permitted to: (1) depress GONZALES's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of GONZALES's face with his eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

Further, law enforcement may compel the use of the biometric features described above if: (1) the procedure is carried out with dispatch and in the immediate vicinity of the premises to be searched, and if, at the time of compulsion, the government has reasonable suspicion as to (2) and (3) infra: (2) that the suspect has committed a criminal act that is the subject matter of the warrant; and (3) reasonable suspicion that the individual's biometric features will unlock the

device, that is, for example, because there is a reasonable suspicion to believe that the individual is the user of the device.

ATTACHMENT A-2

DESCRIPTION OF THE PERSON TO BE SEARCHED

Person to be Searched: **Aaron Paul Gonzales** DOB: [redacted]/1985

ATTACHMENT B-2

DESCRIPTION OF ITEMS TO BE SEIZED

The items to be seized are evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B), and include the following:

1. Records, documents, materials, videos, and photographs, pertaining in any way to child pornography and visual depictions of minors engaged in sexually explicit conduct (hereinafter collectively referred to as "child pornography"), child erotica, and materials pertaining to an interest in child pornography, in whatever format found.

2. Records, documents, materials, and correspondence pertaining to the possession, receipt or distribution of child pornography, and any records indicating whether such was transmitted or received using a computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail.

3. Records, documents, materials, envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, seeking to obtain and/or offering to transmit child pornography through interstate or foreign commerce, including U.S. mail or by computer.

4. Records, documents, materials, envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, identifying persons transmitting or offering to transmit any visual depictions of minors engaged in sexually explicit conduct and any records identifying the means of such transmission.

5. Records, documents, materials, and photographs depicting sexual conduct, whether between adults and minors or between minors.

6. Records, documents, materials evidencing occupancy or ownership of the premises to be searched, including but not limited to, utility bills, mail envelopes, or addressed correspondence.

7. Records, documents, materials or other items which evidence ownership or use of computer and electronic equipment found in the above residence, including but not limited to, sales receipts, bills for Internet access, records containing account/user names and passwords, handwritten notes, and handwritten notes in computer manuals.

8. Records, documents, and materials pertaining to the production, reproduction, receipt, shipment, ordering, soliciting, trading, purchasing, or transactions of any kind involving the transmission through interstate or foreign commerce, including by U.S. mail or other common carrier or by computer or electronic device, of child pornography.

9. Records, documents, and materials, including but not limited to bank, financial, and credit card records, pertaining to the purchase of materials or access to materials containing child pornography.

10. Computer hardware, including central processing units (CPUs), computer software and programs, laptop computers, monitors, keyboards, printers, computer disks (including floppy disks, CDs, DVDs), scanners, disk drives, modems, routers, magnetic storage media, thumb or flash drives, memory sticks, PDAs, digital cameras and memory cards, cell phones, smartphones, I-Phones, I-Pods, I-Pads, electronic notebooks and tablets, hardware and software operating manuals, post-it notes, records containing account/user names and passwords, and other computer-related and/or electronic equipment and/or digital media, to be inspected off-site using appropriate mirror-imaging and other equipment after seizure, which are used as instrumentalities of the crimes noted or which contain any of the items noted in paragraphs 1-9 above.

11. Any of the items described in paragraphs 1-10 above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer or with the aid of computer-related equipment, including floppy diskettes, fixed hard drives, removable hard drives, software, PDAs, cell phones, or memory in any form, to be inspected off-site using appropriate mirror-imaging and other equipment after seizure.

During the execution of this search warrant, law enforcement is permitted to: (1) depress GONZALES's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of GONZALES's face with his eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

Further, law enforcement may compel the use of the biometric features described above if: (1) the procedure is carried out with dispatch and in the immediate vicinity of the premises to be searched, and if, at the time of compulsion, the government has reasonable suspicion as to (2) and (3) infra: (2) that the suspect has committed a criminal act that is the subject matter of the warrant; and (3) reasonable suspicion that the individual's biometric features will unlock the device, that is, for example, because there is a reasonable suspicion to believe that the individual is the user of the device.

ATTACHMENT A-3

SUBJECT PRIUS

DESCRIPTION OF THE VEHICLE TO BE SEARCHED

Vehicle to be Searched: **A green Toyota Prius bearing Virginia license plate OD4080.** The vehicle to be searched is the entire automobile, including all locked containers, compartments, and items therein.

ATTACHMENT B-3

DESCRIPTION OF ITEMS TO BE SEIZED

The items to be seized are evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B), and include the following:

1. Records, documents, materials, videos, and photographs, pertaining in any way to child pornography and visual depictions of minors engaged in sexually explicit conduct (hereinafter collectively referred to as "child pornography"), child erotica, and materials pertaining to an interest in child pornography, in whatever format found.

2. Records, documents, materials, and correspondence pertaining to the possession, receipt or distribution of child pornography, and any records indicating whether such was transmitted or received using a computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail.

3. Records, documents, materials, envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, seeking to obtain and/or offering to transmit child pornography through interstate or foreign commerce, including U.S. mail or by computer.

4. Records, documents, materials, envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, identifying persons transmitting or offering to transmit any visual depictions of minors engaged in sexually explicit conduct and any records identifying the means of such transmission.

5. Records, documents, materials, and photographs depicting sexual conduct, whether between adults and minors or between minors.

6. Records, documents, materials evidencing occupancy or ownership of the premises to be searched, including but not limited to, utility bills, mail envelopes, or addressed correspondence.

7. Records, documents, materials or other items which evidence ownership or use of computer and electronic equipment found in the above residence, including but not limited to, sales receipts, bills for Internet access, records containing account/user names and passwords, handwritten notes, and handwritten notes in computer manuals.

8. Records, documents, and materials pertaining to the production, reproduction, receipt, shipment, ordering, soliciting, trading, purchasing, or transactions of any kind involving the transmission through interstate or foreign commerce, including by U.S. mail or other common carrier or by computer or electronic device, of child pornography.

9. Records, documents, and materials, including but not limited to bank, financial, and credit card records, pertaining to the purchase of materials or access to materials containing child pornography.

10. Computer hardware, including central processing units (CPUs), computer software and programs, laptop computers, monitors, keyboards, printers, computer disks (including floppy disks, CDs, DVDs), scanners, disk drives, modems, routers, magnetic storage media, thumb or flash drives, memory sticks, PDAs, digital cameras and memory cards, cell phones, smartphones, I-Phones, I-Pods, I-Pads, electronic notebooks and tablets, hardware and software operating manuals, post-it notes, records containing account/user names and passwords, and other computer-related and/or electronic equipment and/or digital media, to be inspected off-site using appropriate mirror-imaging and other equipment after seizure, which are used as instrumentalities of the crimes noted or which contain any of the items noted in paragraphs 1-9 above.

11. Any of the items described in paragraphs 1-10 above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer or with the aid of computer-related equipment, including floppy diskettes, fixed hard drives, removable hard drives, software, PDAs, cell phones, or memory in any form, to be inspected off-site using appropriate mirror-imaging and other equipment after seizure.

During the execution of this search warrant, law enforcement is permitted to: (1) depress GONZALES's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of GONZALES's face with his eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

Further, law enforcement may compel the use of the biometric features described above if: (1) the procedure is carried out with dispatch and in the immediate vicinity of the premises to be searched, and if, at the time of compulsion, the government has reasonable suspicion as to (2) and (3) infra: (2) that the suspect has committed a criminal act that is the subject matter of the warrant; and (3) reasonable suspicion that the individual's biometric features will unlock the device, that is, for example, because there is a reasonable suspicion to believe that the individual is the user of the device.

ATTACHMENT A-4

SUBJECT ACCOUNT

DESCRIPTION OF THE ACCOUNT TO BE SEARCHED

This warrant applies to information located within the Google account identified by and/or associated with the email account/address aaronpaulgonzales12@gmail.com which is stored and maintained at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B-4

DESCRIPTION OF ITEMS TO BE SEIZED

ATTACHMENT B

Particular Things to be Seized

I. Information to Be Disclosed by Google LLC (the "Provider")

To the extent that the information described in Attachment A-2 is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held, or maintained inside or outside of the United States, and including any messages, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for the account listed in Attachment A-2 (the GOOGLE ACCOUNT), from the time of the account's creation to the present:

a. The contents of all e-mails and chat communications associated with the GOOGLE ACCOUNT, including stored or preserved copies of e-mails sent to and from the account, email attachments, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the accounts were created, the length of service, the types of service utilized, the IP address used to register the accounts, log-in IP addresses associated with session times and dates, accounts' status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. All records or other information stored by at any time by any individual using the GOOGLE ACCOUNT, including chat logs, address books, contact and buddy lists, calendar data, pictures, videos and files, including in Google Drive, Google Docs, and Google Photos;

d. All records pertaining to communications between the Provider and any person regarding the GOOGLE ACCOUNT, including contacts with support services and records of actions taken; and

e. For all information required to be disclosed under this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant.

Notwithstanding 18 U.S.C. § 2252 or any similar statute or code, the Provider shall provide all responsive data by sending it via U.S. mail, courier, email or the Google LERS Portal

to:

Special Agent John Shields
Homeland Security Investigations
200 Granby Street Suite 600
Norfolk, VA 23510
John.w.shields@ice.dhs.gov

II. Information to Be Seized by the Government

All information described above in Section I that constitutes contraband, fruits, evidence and/or instrumentalities of violations of 18 U.S.C. §§ 2251(a), 2252(a)(2) & (4)(B), including, for the GOOGLE ACCOUNT, information pertaining to the following matters:

a. The identity of the person(s) who created or used the GOOGLE ACCOUNT, including records that help reveal the whereabouts of such person(s);

b. Evidence indicating how and when the GOOGLE ACCOUNT was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

a. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

b. All records pertaining to communications between the Provider and any person regarding the GOOGLE ACCOUNT.

c. Evidence indicating the subscriber or any other individual's state of mind as it relates to the crime under investigation;

d. Any person knowingly receiving, producing, or possessing child pornography, as defined at 18 U.S.C. § 2256(8);

e. Any and all child pornography, meaning any visual depiction including, but not limited to, any photograph, film, video, picture, or computer generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct or such visual depiction appears to be of a minor engaging in sexually explicit conduct;

f. Child erotica materials, including, but not limited to images that may serve to gratify the sexual interest in children that may reveal a sexual preference, or that may evince a criminal intent to commit violations of 18 U.S.C. §§ 2251(a), (a)(2), and (a)(4)(B).

g. Evidence of the times the GOOGLE ACCOUNT was used;

h. Passwords and data security devices, and other access information that may be necessary to access the accounts or identifiers listed on Attachment A-2 and other associated accounts; and

i. Device backups including camera roll and photo stream data to identify child pornography, victims or contraband.